Document Control	
Date Created	07-Feb-2025
Document Author	Information Security Manager
Date Reviewed	04-Mar-2025
Next Review Date	04-Mar-2026
Current Status	Approved
Date Signed Off	06-Mar-2025
Document Classification	Internal Use Only
Retention Period	Perpetual

Version History

Version	Date	Author	Change History
Version 1.0		ISMS Team	Draft Version
Version 2.0		ISMS Team	Version Review & Update

Distribution List

Name	Version	Date
All Staff	Version 2.0	20th March 2025
ISMS Manager	Version 2.0	20th March 2025
CISO	Version 2.0	20th March 2023

Approval List

Name	Position	Signature	Change History
	CEO		

Internal Use Only

This document is subjected to change control.

Internal Use Only

Notice

[redacted] will be referred to as “the organization”.

Internal Use Only

EXECUTIVE SUMMARY

The purpose of this Infrastructure Policy is to establish guidelines for the secure and proper use of organization's

infrastructure while maintaining a culture of openness, trust, and integrity. This policy aims to protect employees, partners, and the company from illegal or damaging actions, whether intentional or unintentional.

All Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts, email services, web browsing, and file transfers, are the property of the organization. These systems must be used strictly for business purposes to serve the interests of the company, clients, and customers. Employees should refer to Human Resources policies for additional details on system usage.

Security is a shared responsibility, requiring the participation and support of every employee and affiliate who interacts with company information and systems. Each computer user must understand and adhere to these guidelines.

Internal Use Only

1.0 PURPOSE

This policy defines the acceptable use of computer equipment at the organization to protect both employees and the company. Unauthorized or inappropriate use may expose the company to security threats, including malware, data breaches, and legal risks.

2.0 SCOPE

This policy applies to all employees, contractors, consultants, temporary staff, and third-party personnel using the organization's infrastructure. It includes all company-owned or leased equipment.

3.0 POLICY

3.1 General Use and Ownership

1. Employees should not expect privacy when using company systems. Management reserves the right to monitor, scan, and review all data on corporate systems at any time.
2. Limited personal use is allowed, such as checking personal emails or reading news, provided it does not interfere with work. Prohibited activities include streaming or downloading videos, movies, or printing e-books using company resources.
3. Authorized IT personnel will continuously monitor equipment, systems, and network traffic per the company's Audit Policy.
4. Regular audits will be conducted to ensure compliance with this policy.

3.2 Security and Proprietary Information

1. All information on company systems should be classified as **confidential** or **non-confidential** according to corporate confidentiality guidelines. Confidential data, including company strategies, trade secrets, customer lists, and research data, must be protected from unauthorized access.
2. Employees must use strong passwords and must not share their credentials. Passwords must be changed every **three months**.
3. All company computers must be secured with a password-protected screensaver that activates after **10 minutes** of inactivity or by logging off.
4. Personal laptops and external storage devices (USB flash drives, external hard drives) are strictly prohibited on company premises.
5. All company-connected devices must run approved antivirus software with up-to-date virus definitions.
6. Employees must exercise caution when opening email attachments from unknown sources to avoid malware threats.

7. Employees must log off their systems before leaving the office. If they must stay logged in, they should set an away message explaining why.
8. Employees are **strictly prohibited** from:
    - Changing computer names
    - Moving or exchanging company computers
    - Installing unauthorized software
9. All hardware and software requests must be emailed to **helpdesk@company.com**.
10. Computers must not be turned off unless explicitly instructed by IT. If done for a specific purpose, an email notification must be sent.
11. Unauthorized files such as personal photos, videos, music, and non-business-related documents will be deleted without notice, and users may be removed from backup services.
12. Employees must use the projector only when meetings involve **three or more people** and must turn it off after use.

3.3 Unacceptable Use

Employees may not engage in any activities that violate **local, state, federal, or international laws** while using company resources. The following activities are strictly prohibited:

System and Network Violations

1. Using or distributing unauthorized software, including pirated copies.
2. Copying or distributing copyrighted material without proper authorization.
3. Exporting software, encryption tools, or technical information in violation of applicable laws.
4. Introducing malicious software such as viruses, worms, or Trojan horses.
5. Sharing account credentials or allowing unauthorized individuals to use company accounts.
6. Using company systems to engage in activities violating harassment or hostile workplace laws.
7. Making fraudulent offers or unauthorized warranty statements.
8. Attempting to breach security systems, access unauthorized data, or disrupt network communications.
9. Conducting unauthorized security scans, port scans, or network monitoring.
10. Bypassing authentication mechanisms or engaging in denial-of-service attacks.
11. Using company resources to send spam, chain emails, or mass communications without proper authorization.

Email and Communication Violations

Kindly refer to the use of email policy

4.0 Enforcement

Employees who violate this policy will be subject to disciplinary action, including but not limited to **warnings, suspension, or termination of employment**.

For any questions regarding this policy, employees should contact the IT Department.

Internal Use Only